(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 029 311 B1

(12) EUROPEAN PATENT SPECIFICATION

(45) Date of publication and mention of the grant of the patent:
27.06.2001 Bulletin 2001/26

(21) Application number: **99912017.3**

(22) Date of filing: **25.03.1999**

(51) Int Cl.[7]: **G07F 7/08**

(86) International application number:
PCT/IE99/00016

(87) International publication number:
WO 99/49424 (30.09.1999 Gazette 1999/39)

(54) CREDIT CARD SYSTEM AND METHOD

KREDITKARTENSYSTEM UND VERFAHREN

SYSTEME ET PROCEDE DE CARTE DE CREDIT

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **25.03.1998 IE 980223**
07.05.1998 IE 980346
15.06.1998 IE 980458
13.07.1998 US 92500 P
26.08.1998 US 98175 P
09.09.1998 US 99614 P
22.01.1999 US 235836

(43) Date of publication of application:
23.08.2000 Bulletin 2000/34

(60) Divisional application:
01201056.7

(73) Proprietor: **Orbis Patents Limited**
Dublin 3 (IE)

(72) Inventors:
- **FLITCROFT, Daniel, Ian**
Sandycove, County Dublin (IE)
- **O'DONNELL, Graham**
Dun Laoghaire, County Dublin (IE)

(74) Representative: **O'Connor, Donal Henry**
c/o Cruickshank & Co.,
1 Holles Street
Dublin 2 (IE)

(56) References cited:
EP-A- 0 081 921
FR-A- 2 661 996
WO-A-97/15893
US-A- 5 721 768

EP 1 029 311 B1

Description

[0001] This invention relates to a credit card system and method, and more particularly, to a credit card system and method offering reduced potential of credit card number misuse.

[0002] The development of retail electronic commerce has been relatively slow in spite of the perceived demand for such trade. The single greatest deterrent to the expansion of retail electronic commerce is the potential for fraud. This potential for fraud has been a major concern for the credit card companies and financial institutions as well as the customers and the providers of the goods and services.

[0003] The former are concerned about fraud because essentially the financial institutions have to bear the initial cost of the fraud. Additionally, the credit card companies have an efficient credit card system which is working well for face to face transactions, i.e., "card present transactions where the credit card is physically presented to a trader and the trader can obtain the credit card number, compare signatures and in many cases photographs before accepting a particular credit card.

[0004] The latter are equally concerned about fraud being well aware that ultimately the user must pay for the fraud. However, there are particular personal concerns for the consumer in that the fraudulent use of the credit card by misuse of the credit card number by a third party may not become apparent for some time. This can happen even if the card is still in his or her possession. Further, when fraud does occur the consumer has the task of persuading the credit card provider that fraud by another did indeed occur.

[0005] There is also the additional fear of being overcharged on a credit card. There are thus particular risks for those credit card holders who have relatively high spending limits, in that if fraud should occur, it may be some considerable time before it is detected. One particular form of fraud referred to as "skimming" is particularly difficult to control. What happens is that the card holder proffers his or her card at an establishment to make a transaction, the relevant information is electronically and/or physically copied from the card and the card is subsequently reproduced. This can be a particular problem with travelers particularly during an extensive period of travel as the fraudulent card may tum up in other places and it may be some considerable time before the fraud is detected.

[0006] For remote credit card use, the credit card holder has to provide details of name, master credit card number, expiration date and address and often many other pieces of information for verification; the storing and updating of the information is expensive but necessary, This of itself is a considerable security risk as anybody will appreciate that this information could be used to fraudulently charge goods and services to the card holder's credit card account. Such fraudulent use is not limited to those people to whom the credit card information has been given legitimately, but extends to anybody who can illegitimately obtain such details. A major problem in relation to this form of fraud is that the credit card may still be in the possession of the legitimate holder as these fraudulent transactions are taking place. This is often referred to as "compromised numbers" fraud. Indeed all this fraud needs is one dishonest staff member, for example in a shop, hotel or restaurant, to record the credit card number. It is thus not the same as card theft.

[0007] The current approaches to the limiting of credit card fraud are dependent on the theft of a card being reported and elaborate verification systems whereby altered patterns of use initiate some enquiry from the credit card company. Many users of credit cards have no doubt received telephone calls, when their use of the card has been exceptional, or otherwise unusual in the eyes of the organization providing the verification services.

[0008] Thus, there have been many developments in an effort to overcome this fundamental problem of fraud, both in the general area of fraud for ordinary use of credit cards and for the particular problems associated with such remote use.

[0009] One of the developments is the provision of smart cards which are credit card devices containing embedded electronic circuitry that can either store information or perform computations. Generally speaking they contribute to credit card security systems by using some encryption system. A typical example of such a smart card is disclosed in U.S. Patent No. 5,317,636 (Vizcaino).

[0010] Another one of the developments is the Secure Electronic Transaction (SET) protocol which represents the collaboration between many leading computer companies and the credit card industry which is particularly related to electronic transmission of credit card details and in particular via the Internet. It provides a detailed protocol for encryption of credit card details and verification of participants in an electronic transaction.

[0011] Another method that is particularly directed to the Internet is described in U.S. Patent No. 5,715,314 (Payne et al.). U.S. Patent 5,715,314 discloses using an access message that comprises a product identifier and an access message authenticator based on a cryptographic key. A buyer computer sends a payment message that identifies a particular product to a payment computer. The payment computer is programmed to receive the payment message, to create the access message, and to send the access message to a merchant computer. Because the access message is tied to a particular product and a particular merchant computer, the access message can not be generated until the user sends the payment message to the payment computer. Because the access message is different from existing credit card formats, the access message is ill-suited for phone/mail orders and other traditional credit card transactions.

[0012] There are then specific electronic transaction